UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,481	11/17/2003	Simon Charles Watt	550-481	6834

23117 7590 05/16/2006

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
FLOURNOY, HORACE L	
ART UNIT	**PAPER NUMBER**
2189	

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/714,481	WATT, SIMON CHARLES	
	Examiner	Art Unit	
	Horace L. Flournoy	2189	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *3/6/2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/19/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This Office action has been issued in response to amendment filed 6 March 2006. Claims 1-20 are pending. Applicant's arguments have been carefully and respectfully considered, but they are not entirely persuasive, as will be discussed in more detail below, even in light of the instant amendments. Accordingly, this action has been made FINAL.

ACKNOWLEDGEMENT OF REFERENCES CITED BY APPLICANT

As required by **M.P.E.P.** 609(c), the applicant's submission of the Information Disclosure Statement dated **04/19/2006** is acknowledged by the examiner. As required by **M.P.E.P.** 609(c), a copy of the PTOL-1449 is attached to the instant office action. The examiner did not initial the section of the IDS labeled "Other Documents". The applicant failed to cite the inventor and the filing date of these related U.S. applications (See M.P.E.P. 609.04 (a)).

Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

REJECTIONS BASED ON PRIOR ART

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by **Gardner et al. (U.S. PG PUB No. 2003/0101322 hereafter referred to as Gardner) with Microsoft Computer Dictionary, 5th edition, © 2002, page 81 offered as extrinsic evidence.**

[Note: the usage by the applicant of the word "*operable*" may not positively recite the limitations that follow ("a processor *operable*...", "...each entry being *operable*...", and "the memory unit is *operable*..."). See the limitations below.]

With respect to independent **claims 1 and 11**,

> *"A data processing apparatus, comprising: a processor* **[FIG. 3, element 32]** *operable in a plurality of modes* **["user processes"]** *and a plurality of domains,"* **[Gardner discloses in paragraph [0189], "secure and non-secure".]** *said plurality of domains comprising a secure domain and a non-secure domain* **[Gardner discloses in paragraph [0189], "secure and non-secure" (Also see paragraph [0033])]** *said plurality of modes* **["user processes"]** *including at*

least one non-secure mode being a mode in the non-secure domain **["secure and non-secure user processes"]** *and at least one secure mode being a mode in the secure domain* **["secure and non-secure user processes]. Gardner discloses in paragraph [0062], "...when processor 32 is implemented as an IA-64 processor, processor privilege level, region IDs, protection keys, and page access rights are primitives upon which domains and processes are protected from one another in SPA 30"]**

"...said processor being operable such that when executing a program in a secure mode **[Gardner discloses in paragraph [0189], a "secure user process"]** *said program has access to secure data which is not accessible when said processor is operating in a non-secure mode***[Gardner discloses in paragraph [0062], "domains and processes are protected from one another in SPA 30" (Also see paragraph [0189])]**;"

"...a memory unit **[FIG. 3, element 20]** *comprising a plurality of entries* **[FIG. 3, elements 140, 142]** *and operable to store data required by the processor, each entry being operable to store one or more data items consisting of either secure data or non-secure data* **[paragraph [0189]]**,"

"...and a flag **[paragraph [0189], "bit"]** *being associated with each entry in the memory unit* **["...secure user processes are distinguished from non-secure user processes by setting a bit in the "magic number" or ELF (Executable and Linkable Format) header. With respect to this limitation, Gardner teaches each entry has a header.]** *to store a value indicating whether the one or more data items stored in the associated entry are said secure data or said non-secure data* **["the information for distinguishing between secure and**

non-secure user processes is contained in a secure memory page in memory 74."];"

"...when the processor is operating in said at least one non-secure mode **[Gardner discloses in paragraph [0189], "Non-secure user processes"]**, *the memory unit being operable, upon receipt of a memory access request issued by the processor when access to an item of data is required, to prevent access to any data item within an entry of the memory unit that the associated flag indicates has secure data stored therein."* **[Gardner discloses in paragraph [0026], "Secure platform 40, however, ensures that one domain cannot accidentally or intentionally access another domain's memory." With respect to this limitation, Gardner teaches that if the secure platform detects if the memory access request is seeking to access the secure memory of the further memory unit, then the secure platform prevents that access (ensures that one domain cannot...access)]**

With respect to **claims 2 and 12**,

*"A data processing apparatus as claimed in claim 1***[see rejection of claim 1]**, *wherein the memory unit* **[FIG. 3, element 36]** *is a cache* **[paragraph [0157], "If the number of active protection keys is greater than the available protection key registers 118, SPK employs the protection key registers as a cache..."]**, *and each said entry is a cache line of the cache."* **[The examiner cites the definition of "cache" from Microsoft Computer Dictionary, 5th edition, page 81]**

With respect to **claims 3 and 13**,

"A data processing apparatus as claimed in claim 1 **[see rejection of claim 1]**, *wherein the memory unit* **[FIG. 3, element 20]** *is coupled to the processor* **[FIG. 3, element 32]** *via a processor bus* **(see connection of elements 20 and 32 as shown in FIG. 3)**,"

"...the memory unit and processor forming a device **[Gardner discloses in paragraph [0002], "Computer systems include at least one processor and memory."]**

"...and the data processing apparatus further comprises a device bus via which the device is connectable to a further memory unit **[Gardner discloses in FIG.3, a processor (element 32), a cache (element 118), and a further memory unit (element 20). Furthermore, Gardner also discloses in paragraph [0003], "...The Intel Architecture (IA-64) and the HP Precision Architecture (PA-RISC) type processors..." With respect to this limitation, it is notoriously well known that the Intel Architecture (IA-64) and the HP Precision Architecture (PA-RISC) comprises a device bus via which the devices are connectable to a further memory unit(s)]**,"

"...the further memory unit having secure memory for storing secure data and non-secure memory for storing non-secure data. **[paragraph [0189]]** "

With respect to **claims 4 and 14**,

"A data processing apparatus as claimed in claim 3 **[see rejection of claim 3]**, *wherein if the memory access request* **[paragraph [0026], "access...memory"]** *specifies a data item that is not stored within the memory unit, the memory*

access request is output on to the device bus to cause that data item to be accessed in the further memory unit **[Gardner discloses in paragraph [0057], "If the required translation entry 214 is not stored in TLB 128, in one embodiment processor 32 can also optionally search a virtual hash page table (VHPT) 142 (shown in FIG. 3) in memory 74]**, *the data processing apparatus further comprising:"*

"...partition checking logic connected to the device bus **[SPK of FIG. 3, element 36]** *and operable, whenever the memory access request is issued by the processor when operating in said at least one non-secure mode and is output onto the device bus, to detect if the memory access request is seeking to access the secure memory of the further memory unit, and upon such detection to prevent the access specified by that memory access request."* **[Gardner discloses in paragraph [0026], "Secure platform 40, however, ensures that one domain cannot accidentally or intentionally access another domain's memory." With respect to this limitation, Gardner teaches that if the secure platform detects if the memory access request is seeking to access the secure memory of the further memory unit, then the secure platform prevents that access (ensures that one domain cannot...access)]**

With respect to **claims 5 and 15**,

"A data processing apparatus as claimed in claim 4 **[see rejection of claim 4]**, *wherein if the memory access request* **[paragraph [0026]]** *specifies a data item that is not stored within the memory unit, then if the partition checking logic* **[SPK of FIG. 3, element 36]** *determines that the processor is allowed to access that*

data item **[paragraph [0021]]**, *that data item is retrieved from the further memory unit and stored in one of said entries of the memory unit* **[Gardner discloses in paragraph [0021], "...then that memory page can be accessed at all levels]** , *the value to be set for the flag associated with that entry being indicated by the partition checking logic***[paragraphs [0189] and [0146]]**" **(Also see rejection of claims 3 and 4)**.

With respect to **claims 6 and 16**,

"*A data processing apparatus as claimed in claim 3***[see rejection of claim 3]**, *wherein the further memory unit is a main memory of the data processing apparatus* **[FIG. 3, element 20]**." **(Also see rejection of claims 3 and 13)**.

With respect to **claims 7 and 17**,

"*A data processing apparatus as claimed in claim 1***[see rejection of claim 1]**, *wherein the flag* **[paragraph [0189]: "...a bit in the "magic number" or ELF (Executable and Linkable Format) header]** *is contained within the memory unit* **[paragraph [0189]: "contained in a secure memory page in memory 74]** *and comprises a single bit set to indicate whether the associated entry has secure data or non-secure data stored therein* **[paragraph [0189]: "distinguishing between secure and non-secure user processes"]**.

With respect to **claims 8 and 18**,

"*A data processing apparatus as claimed in claim 1***[see rejection of claim 1]**, *wherein the memory unit is operable to issue an abort signal* **[paragraph [0191]:**

"flushed from protection key registers"] *if the processor, whilst operating in said at least one non-secure mode* **[paragraph [0191]: "outside of the secure user process"]**, *seeks to access any data item within an entry of the memory unit that the associated flag indicates has secure data stored therein* **[paragraph [0026]: "Secure platform 40, however, ensures that one domain cannot accidentally or intentionally access another domain's memory." Gardner teaches that the processor cannot access secure memory while in non-secure mode]** (Also see claim 1 rejection).

With respect to **claims 9 and 19**,

*"A data processing apparatus as claimed in claim 1***[see rejection of claim 1]**, *wherein the processor* **[FIG. 3, element 32]** *is coupled to the memory unit* **[FIG. 3, element 20]** *via a memory management unit* **[SPK 36; FIG. 3, element 36]**..." *"...operable, upon receipt of the memory access request* **[paragraph [0134]]**, *to perform one or more predetermined access control functions* **[paragraph [0134]: allocate, map, unmap, and free virtual addresses]** *to control issuance of the memory access request to the memory unit* **[paragraph [0134]: SPK 36 manages the details behind the virtual addresses]**."

With respect to **claims 10 and 20**,

"A data processing apparatus as claimed in claim 9 **[see rejection of claim 9]**, *wherein the memory access request specifies a virtual address* **[paragraphs [0049] and [0055]]**," (See also **FIGs. 3, 4 and 5**).

"...and one of said predetermined access control functions comprises conversion of the virtual address to a physical address **[paragraph [0056]]**." (See also **FIGs. 4 and 5**).

ACKNOWLEDGMENT OF ISSUES RAISED BY THE APPLICANT

Response to Amendment

Applicant's arguments filed **March 6, 2006** have been fully considered but they are not deemed to be persuasive and, as required by **M.P.E.P. 707.07(f)**, a response to these arguments appears below.

ARGUMENTS CONCERNING FORMAL MATTERS

The applicant's traversal of the formal requirements requested by the examiner is addressed in the following section as required by **M.P.E.P. 707.07(f).**

ARGUMENTS CONCERNING PRIOR ART REJECTIONS

1ST POINT OF ARGUMENT:

With respect to the arguments on page 8, line 16 of the applicant's remarks, the examiner respectfully disagrees. Paragraph [0189] of Gardner teaches "secure and non-secure" domains. The examiner interprets "secure and non-secure" as "a plurality of domains".

2ND POINT OF ARGUMENT:

With respect to the argument on page 9, line 4 of the applicant's remarks, the applicant merely alleges that Gardner's protection domains are quite different to the claimed domains, and therefore the arguments are not persuasive. Furthermore the examiner believes that Gardner does teach, "wherein when the processor is in the secure domain, a program executed by the processor has access to secure data which is not accessible from the non-secure domain" e.g. in paragraph [0189]. Therefore, the examiner respectfully disagrees with the applicant's argument.

3rd POINT OF ARGUMENT:

With respect to the argument on page 9, line 18 of the applicant's remarks, the applicant merely alleges that Gardner's "setting a bit" is different to the claimed "flag", and therefore the arguments are not persuasive. The examiner interprets the "bit" in the header, which can be set as disclosed by Gardner is indeed used as a "flag". This "bit" which can be set distinguishes from non-secure and secure "data" or data within user processes. Therefore, the examiner respectfully disagrees with the applicant's argument.

4th POINT OF ARGUMENT:

With respect to the argument on page 10, line 2 and line 16 of the applicant's remarks, the examiner respectfully disagrees with the applicant's argument. Gardner discloses in paragraph [0189], "In one embodiment, the information for distinguishing between secure and non-secure user processes is contained in a secure memory page in memory 74."

5th POINT OF ARGUMENT:

With respect to the argument on page 11, line 7 of the applicant's remarks, the examiner apologizes for any confusion. The examiner cited element 20 and paragraph [0157]. Paragraph [0157] explicitly cites that element 36 is within element 20 and as a cache. Furthermore the definition of "cache" is cited as extrinsic evidence by the examiner as stated supra.

Also with respect to the applicant's remarks on page 11, line 10, refer to claim 13 of Gardner. The examiner also points the applicant to the fact that these limitations are not found within the applicant's claims.

CONCLUSION

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Direction of Future Correspondences

Any inquiry concerning this communication or earlier communication from the examiner should be directed to Horace L. Flournoy whose telephone number is (571) 272-2705. The examiner can normally be reached on Monday through Friday 8:00 AM to 5:30 PM (ET).

Important Note

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Reginald G. Bragdon can be reached on (571) 272-4204. The fax phone numbers for the organization where this application or proceeding is assigned is (703) 746-7239.

Information regarding the status of an Application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or PUBLIC PAIR. Status information for unpublished applications is available through Private Pair only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Reginald G. Bragdon
REGINALD G. BRAGDON
PRIMARY EXAMINER

Horace L. Flournoy
Patent Examiner
Art unit: 2189

Supervisory Patent Examiner
Technology Center 2100